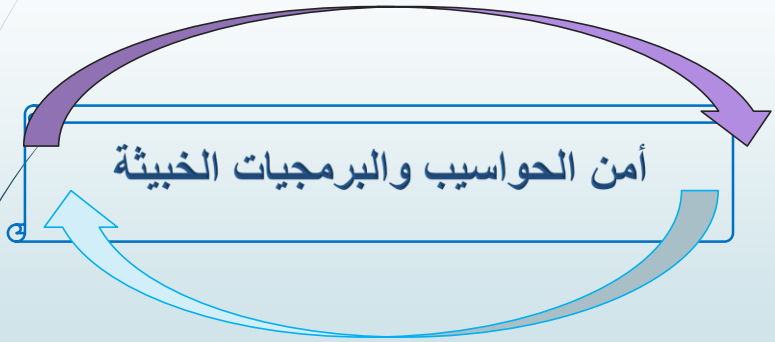
أمن المعلومات

GS224-7



امن الحواسيب

يقصد بأمـن الحاسبات هنا، أمن أجهـزة الحاسب الآلي(كعتاد صلـد)، ويقصد بأمن البرمجيات أمن أنظمة التشغيل التي تتحكم بالأجهزة، وأمن البرامج التطبيقيّة التي يتعامل معها المستخدم لأداء مهامه اليومية، ويقصد بأمن الملفّات أمن الملفّات نفسها كأوعية لتخزين المعلومات، مثل: ملفات معالجة النصوص، والجداول الإلكترونيّة، وقواعد البيانات، ورسائل البريد الإلكتروني، وأمن نظام الملفّات(File System) الذي يتحكم بإدارة جميع الملفّات.

التهديدات الرقمية للحواسيب و البرمجيات و الملفات

يكمن التهديد الرئيس لجهاز الحاسب الآلي(الصلد) في وفرته. فالجهاز هو أكثر المناطق ضعفًا في مواجهة الهجمات، وأكثرها طاعة لضوابط الرقابة التلقائية. وتشمل تهديدات أجهزة الحاسب الآلي كذلك: السرقة، وإلحاق الضرر بها سواءً عن طريق الخطأ أم العمد.

إنّ انتشار أجهزة الحاسبات الشخصية والاعتماد عليها في إنجاز كثير من الأعمال، والزيادة المطّردة في استخدام شبكات الحاسب الآلي، زادت من احتمالات فقد الأجهزة. لذلك فإنّ الاحتياطات الأمنيّة الماديّة(الفيزيقية) والإداريّة ضرورية للتعامل مع تلك التهديدات.

يكمن التهديد الرئيس للبرمجيات في الهجمات على توفر البرنامج، خاصّة البرامج التطبيقيّة، حيث غالبًا ما تكون سهلة الحذف، ومن التهديدات كذلك تغيير البرامج التطبيقيّة أو إتلافها؛ لتصبح غير مفيدة. ومن أكثر المشكلات التي يجب التعامل معها في مجال البرمجيات هو التعديلات التي تحدث في البرنامج الذي لا يزال يعمل، لكنه يجري تحديثه بطريقة مختلفة عن الطريقة السابقة. ولحل هذه المشكلة يجب توزيع البرامج بعناية عن طريق إنشاء النسخ وفق إصدارات تدريجية، وتوزيع النسخ الأحدث منها. المشكلة الأخيرة التي تواجه البرمجيات هي الخصوصية، ومع أن هنالك كثيرًا من الاحتياطات التي اتخذت، إلّا أنّ مشكلة النسخ غير المرخّص له للبرامج ما زالت بدون حل.

التهديدات الرقمية للحواسيب و البرمجيات و الملفات

إنّ التهديدات الأمنيّة بخصوص البيانات واسعة جدًا لدرجة أنها تشمل تهديدات توفرها وتهديدات سرّيّتها، وتهديدات سلامتها وتكاملها. ففي حالة التوفر، فإنّ التهديدات تكمن في إتلاف ملفات البيانات، التي قد تحدث إمّا عن طريق الخطأ أو بشكل متعمّد، وفي حالة السِّريّة، تكمن التهديدات في القراءة غير المسموح بها لملفات البيانات أو قواعد البيانات، وفي حالة سلامة البيانات وتكاملها، تكمن التهديدات في تغيير البيانات، إمّا بحذف أو إضافة أو تعديل، وهذا المجال قد أضحى أكثر المجالات اهتمامًا بالأبحاث والجهود المبذولة من جانب المختصين في أمن المعلومات. وهناك تهديد آخر لكنه أقل ظهورًا، وهو تحليل البيانات وتحليل تصاميم قواعد البيانات من أجل كسر حمايتها، ويمكن القول إن سلامة البيانات هي الهاجس الأكبر في معظم المنشآت؛ لأن التعديلات التي تجرى على ملفات البيانات قد تترتب عليها نتائج تتراوح بين المخاطر الصغيرة إلى المخاطر الكارثية.

1- البرامج الضارة (Malware)

هو مصطلح جديد نسبيًا في مجال الأمان. وقد استخدم هذا المصطلح للحاجة إلى مناقشة البرامج أو التطبيقات التي صمّمت خصّيصًا بحيث تحتوي مهام اختراق الأنظمة، وكسر سياسات الأمان وخططه، أو القيام بأعمال ماكرة أو عمليّات مدمّرة. ولأنّ هذا النوع من البرامج قد بدأ يأخذ أشكالًا كثيرة مختلفة، مثل: الأبواب الخلفية، وخدع البيانات، ونشر مانعات الخدمة(Deny of Service-DoS)، وحصان طروادة، والفيروسات، والديدان، لذا فإنّ هذا التعبير أصبح يستخدم لمجموعة كبيرة من البرامج الضارّة، والمخادعة، والماكرة.

رغم أنّ مصطلح "البرامج الضارّة" عادة ما يستخدم بطريقة عمومية؛ ليكون مرادفًا للفيروس، إلا أنه بنفس الطريقة أصبح يطلق اسم "فيروس" ببساطة لوصف أي نوع من مشكلات الحاسب الآلي؛ مما سبب بعض اللبس وصعوبة التفريق بين أنواع البرامج الضارة. ولم يقف الأمر عند ذلك الحد، بل أصبح هناك خلط واضح بين الفيروسات، والديدان، وأحصنة طروادة، رغم أن لكل منها خصائصه التي تميزه من غيره، وإن كان القاسم المشترك بينها هو إلحاق الضرر.

1- البرامج الضارة (Malware)

أكثر أنواع التهديدات تطورا لأنظمة الحاسب تتم من خلال البرامج التي تستغل نقاط الضعف في أنظمة الحوسبة. يشار إلى هذه التهديدات على أنها **برامج خبيثة أو ضارة** (**Malicious Software**) .

- يمكن تقسيم البرامج الخبيثة إلى فئتين:
  - البرامج (او أجزاء من برنامج) التي تحتاج إلى **برامج مضيفة :** أجزاء من البرنامج (او برنامج) لا يمكن أن توجد بشكل مستقل فعليا عن البرنامج التطبيقي، أو برنامج النظام. ومن الأمثلة على ذلك الفيروسات والقنابل المنطقية والأبواب الخلفية.
  - **برامج مستقلة** قائمة بذاتها : البرامج المستقلة هي التي يمكن جدولتها وتشغيلها بواسطة نظام التشغيل. من الأمثلة على ذلك برامج الديدان.
- وتقسم أيضًا بناً على **الاضرار التي تسببها** البرامج الخبيثة فمنها التي لا تتضاعف وتلك التي تتضاعف.
  - الاضرار التي **لا تتضاعف** تسببها برامج أو أجزاء من البرامج التي يتم تنشيطها بواسطة مشغل. ومن الأمثلة القنابل المنطقية والأبواب الخلفية وبرامج الروبوت.
  - الاضرار التي **تتضاعف** تسببها برامج مستقل أو أجزاء من البرامج قد ينتج عند تنفيذه نسخة واحدة أو أكثر من نفسه ليتم تفعيلها لاحقًا على نفس النظام أو على نظام آخر. من الأمثلة على ذلك الفيروسات والديدان.
- تعتبر تهديدات متطورة لأنظمة المعلومات .

مصطلحات البرمجيات الضارة

- **الفيروس:** يلحق نفسه ببرنامج وينشر نسخًا منه على برامج أخرى (**Virus**).
- **الدودة:** برنامج ينشر نسخًا من نفسه على أجهزة حاسوب أخرى (**Worm**).
- **القنبلة المنطقية:** تطلق فعل ما (تنفجر) عند حدوث شرط ما (**Logic bomb**).
- **حصان طروادة:** برنامج يحتوي على وظائف إضافية غير متوقعة (**Trojan horse**).
- **الباب الخلفي:** تعديل في البرنامج يسمح بالوصول غير المصرح به إلى وظائفه (**Backdoor**).
- **برنامج متنقل:** برنامج يمكن وضعه دون تغيير على مجموعة غير متجانسة من المنصات البرمجية وتنفيذه باستخدام دلالات متطابقة (**Mobile code**).
- **الادوات التلقائية** (مولد الفيروسات): مجموعة من ادوات القرصنة الخبيثة لتوليد فيروسات جديدة تلقائيًا و تستخدم لاقتحام حواسيب جديدة عن بُعد (**Auto-rooter Kit**).
- **برامج الرسائل الاقتحامية**: تُستخدم لإرسال كميات كبيرة من البريد الإلكتروني غير المرغوب فيه ، أو لمهاجمة الأنظمة التي تحتوي على عدد كبير من حركة المرور لتنفيذ هجوم تعطيل الخدمة (**Spammer and flooder programs**).
- **مسجل المفاتيح:** يلتقط ضغطات مفاتيح لوحة الادخال على النظام المخترق (**Keyloggers**).
- **الأدوات المصدرية:** مجموعة من أدوات القرصنة المستخدمة بعد اختراق المهاجم لنظام حاسب واكتسب وصولاً على مستوى الجذر/الأساس (**Rootkit**).
- **الزومبي:** برنامج على الجهاز المصاب يتم تفعيله لشن هجمات على اجهزة اخرى (**Zombie**).

مصطلحات البرمجيات الضارة

- **الحمولة:** افعال البرمجيات الخبيثة (Payload).
- **البرمجيات الاجرامية:** مجموعات الأدوات لبناء وانتاج برمجيات الخبيثة ؛ تشمل آليات النشر والضرر المفتعل (Crimeware).
  - Zeus, Sakura, Blackhole, Phoenix
- **التهديدات المستمرة المتقدمة** (Advanced Persistent Threats)
  - متقدم: متطورة
  - مستمر: هجوم مستمر لفترة طويلة من الزمن
  - التهديد: أهداف محددة (مهاجمون قادرون وممولون جيدًا)

1- البرمجيات الضارة : أ - الفيروسات

فيروس الحاسب الآلي هو برنامج يُعدُّ لينسخ وينشر نفسه، وينتشر ذاتيًّا دون علم وتعاون مع المالك أو المستخدم للجهاز، ولم يتم التوصل بعد لتعريف موحد للفيروسات متفق عليه من الباحثين كافّة، والتعريف العام هو تعريف فريد كوهين[1]، الذي يعرّف الفيروس بأنه: «برنامج يعدّل البرامج الأخرى لكي تحتوي نسخة معدّلة من نفسها» ورغم أنّ هذا التعريف يصف جُلّ الفيروسات، وأن كثيرًا من الباحثين ما زالوا يصرّون على استخدامه، إلّا أنّه يقتصر على البرامج التي تقحم نفسها بنفسها في البرامج الأخرى فقط، وهو بذلك يهمل كثيرًا من الفيروسات التي تقحم نفسها في الملفّات التي ليست برامج بطبيعتها، كالوثائق مثلًا. وعليه

" برنامج يتم إدراجه في نظام ، سرًا عادةً ، بقصد المساس بسرية أو نزاهة أو توفر بيانات الضحية أو تطبيقاته أو نظام تشغيله أو خلاف ذلك كإزعاج الضحية أو مضايقته."

1- البرمجيات الضارة : أ - الفيروسات

يمر الفيروس النموذجي خلال حياته بالمراحل الأربع التالية:

- **مرحلة الخمول**: يكون الفيروس خاملاً. ويتم تنشيط الفيروس من خلال حدث ما ، مثل تاريخ ، أو وجود برنامج أو ملف آخر ، أو تجاوز سعة القرص لحد ما. ليست كل الفيروسات لديها هذه المرحلة.
- **مرحلة الانتشار**: يضع الفيروس نسخة متطابقة منه في برامج أخرى أو في مناطق معينة للنظام على القرص. سيحتوي كل برنامج مصاب الآن على نسخة من الفيروس ، والتي ستدخل بدورها مرحلة الانتشار.
- **مرحلة التحفيز**: يتم تنشيط الفيروس لأداء الوظيفة التي تم تصميمه من أجلها. كما هو الحال مع مرحلة الخمول ، يمكن أن تحدث مرحلة التحفيز بسبب مجموعة متنوعة من أحداث النظام ، بما في ذلك عدد المرات التي قامت فيها هذه النسخة من الفيروس من نسخ نفسها.
- **مرحلة التنفيذ**: يتم تنفيذ الوظيفة والتي قد تكون غير ضارة ، على سبيل المثال رسالة على الشاشة ، أو إتلاف ، على سبيل المثال إتلاف البرامج وملفات البيانات.

1- البرمجيات الضارة : أ - الفيروسات : البنية

- يتكون فيروس الحاسوب من ثلاثة مكونات:
  - **آلية العدوى**: الوسيلة التي ينتشر بها الفيروس بحيث يمكنه التكاثر. يشار إلى الآلية أيضًا باسم ناقل العدوى.
  - **التحفيز**: حدث أو حالة ما تحدد متى يتم تنشيط الحمولة أو توزيعها.
  - **الحمولة**: ما يفعله الفيروس إلى جانب انتشاره. قد تنطوي الحمولة على تلف أو قد تتضمن نشاطًا غير خطر ولكن ملحوظًا.
- **الفيروس في المقدمة أو النهاية** نسبة إلى البرنامج المنفذ ، أو يمكن تضمينه بطريقة أخرى. مفتاح تشغيله هو أن البرنامج المصاب عند استدعائه ، سيقوم أولاً بتنفيذ شفرة الفيروس ثم تنفيذ شفرة البرنامج المنفذ.
- بمجرد دخول الفيروس إلى النظام عن طريق إصابة برنامج ما بالنظام ، يكون في وضع يمكنه من **إصابة بعض أو جميع الملفات** القابلة للتنفيذ الأخرى على هذا النظام عند تنفيذ البرنامج المصاب. وبالتالي ، يمكن منع العدوى الفيروسية تمامًا عن طريق منع الفيروس من الدخول للنظام في المقام الأول.
- لسوء الحظ ، **الوقاية صعبة للغاية** لأن الفيروس يمكن أن يكون جزءًا من أي برنامج خارج النظام. وبالتالي ، ما لم يكتف المرء بكتابة جميع برامج النظام والتطبيق الخاصة به ، يكون المرء عرضة للخطر.
- يعد **الافتقار إلى ضوابط الوصول** على أجهزة الحاسوب القديمة أحد الأسباب الرئيسية للانتشار السريع للفيروسات التقليدية القائمة على شفرة الآلة على هذه الأنظمة. في المقابل ، في حين أنه من السهل كتابة فيروس شفرة الآلة لأنظمة يونيكس (UNIX)، إلا أنها غير فعالة تقريبًا عمليا نظرًا لوجود ضوابط في الوصول إلى هذه الأنظمة منعت الانتشار الفعال للفيروس.

1- البرمجيات الضارة : أ - الفيروسات : البنية

يوضح الشكل التصور العام لبنية الفيروس.

- في هذه الحالة ، شفرة الفيروس (V) ملحقة في مقدمة البرنامج المصاب ، ويُفترض أن نقطة الدخول إلى البرنامج ، عند استدعائه ، هي السطر الأول من البرنامج.

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

1- البرمجيات الضارة : أ - الفيروسات : البنية

- يبدأ البرنامج المصاب ببرنامج الفيروس ويعمل على النحو التالي. السطر الأول من التعليمات البرمجية هو القفزة إلى برنامج الفيروسات الرئيسي.
- السطر الثاني عبارة عن علامة خاصة يستخدمها الفيروس لتحديد ما إذا كان برنامج الضحية المحتمل قد أصيب بالفعل بهذا الفيروس أم لا. عندما يتم استدعاء البرنامج ، يتم نقل التحكم على الفور إلى برنامج الفيروسات الرئيسي. يبحث برنامج الفيروسات أولاً عن الملفات القابلة للتنفيذ غير المصابة ويصيبها.
- بعد ذلك ، قد يقوم الفيروس ببعض الإجراءات ، وعادة ما تكون ضارة بالنظام. يمكن تنفيذ هذا الإجراء في كل مرة يتم فيها استدعاء البرنامج ، أو يمكن أن يكون قنبلة منطقية لا يتم تشغيلها إلا في ظل ظروف معينة.
- أخيرًا ، ينقل الفيروس التحكم إلى البرنامج الأصلي. إذا كانت مرحلة إصابة البرنامج سريعة ، فمن غير المرجح أن يلاحظ المستخدم أي فرق بين تنفيذ برنامج مصاب وغير مصاب.

1- البرمجيات الضارة : أ - الفيروسات : البنية

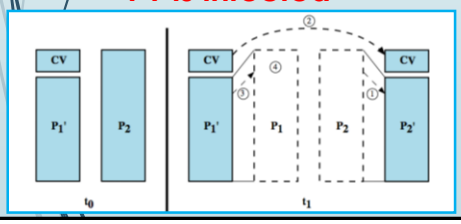
```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
       (1)     compress file;
       (2)     prepend CV to file;
       }

main:   main-program :=
          {if ask-permission then infect-executable;
       (3)     uncompress rest-of-file;
       (4)     run uncompressed file;}
       }
```

P1 is infected



ضغط الفيروسات

- يمكن اكتشاف فيروس مثل الفيروس الموصوف سابقا بسهولة لأن النسخة المصابة من البرنامج أطول من النسخة غير المصابة.
- تتمثل إحدى طرق إحباط مثل هذه الوسيلة البسيطة لاكتشاف الفيروس في ضغط الملف القابل للتنفيذ بحيث يكون كل من النسختين المصابة وغير المصابة بطول متطابق. توضح الشفرة في الشكل التالي بشكل عام المنطق المطلوب.

1- البرمجيات الضارة : أ - الفيروسات : البنية

ضغط الفيروسات

تم ترقيم الخطوط الرئيسية في هذا الفيروس كما ان الشكل السابق يوضح العملية. في هذا المثال ، لا يقوم الفيروس بأي شيء سوى الانتشار. كما في المثال السابق ، قد يحتوي الفيروس على قنبلة منطقية. نفترض أن البرنامج (P1) مصاب بالفيروس (CV) ، وعند استدعاء هذا البرنامج ينتقل التحكم الى الفيروس المصاب به ، والذى سيقوم بالخطوات التالية:

1. لكل ملف (P2) غير مصاب يتم العثور عليه ، يقوم الفيروس أولاً بضغط هذا الملف لإنتاج نسخة مضغوطة ، وهي أقصر من البرنامج الأصلي من حيث حجم الفيروس.
2. يتم وضع نسخة من الفيروس في مقدمة البرنامج المضغوط.
3. يفك ضغط النسخة المضغوطة من البرنامج الأصلي المصاب .
4. يتم تنفيذ البرنامج الأصلي غير المضغوط.

1- البرمجيات الضارة : أ - الفيروسات : التصنيف

كان هناك سباق تسلح مستمر بين كتاب الفيروسات وكتاب برامج مكافحة الفيروسات منذ ظهور الفيروسات لأول مرة. كلما تم تطوير إجراءات مضادة فعالة للأنواع الموجودة من الفيروسات تم تطوير أنواع جديدة من الفيروسات

- يشمل تصنيف الفيروسات **حسب الهدف** ما يلي:
  - **مصيبي قطاع الاقلاع**: يصيب سجل الإقلاع الرئيسي أو سجل إقلاع ، وينتشر عند إقلاع نظام من القرص الذي يحتوي على الفيروس.
  - **مصيبي الملفات**: يصيب الملفات التي يعتبرها نظام التشغيل قابلة للتنفيذ.
  - **فيروس الماكرو**: يصيب الملفات ذات التعليمات البرمجية للماكرو والتي يتم تفسيرها بواسطة أحد التطبيقات.
  - **متعدد الأجزاء**: يصيب بطرقً متعددة
- يشمل تصنيف الفيروسات **حسب استراتيجية الإخفاء** ما يلي:
  - **فيروس مشفر**: يقوم الفيروس بإنشاء مفتاح تشفير عشوائي ، يتم تخزينه مع الفيروس ، ويقوم بتشفير ما تبقى من الفيروس. عندما يتم استدعاء البرنامج المصاب ، يستخدم الفيروس المفتاح العشوائي المخزن لفك تشفير الفيروس. عندما يتكاثر الفيروس يتم تحديد مفتاح عشوائي مختلف.
  - **فيروس التخفي**: نوع من الفيروسات مصمم بشكل صريح لإخفاء نفسه من الكشف عن طريق برامج مكافحة الفيروسات. وبالتالي ، يتم إخفاء الفيروس بأكمله ، وليس مجرد الحمولة. (على سبيل المثال ، ضغط)
  - **فيروس متعدد الأشكال**: فيروس يتحول مع كل إصابة ، مما يجعل اكتشافه من خلال "توقيع" الفيروس مستحيلاً.
  - **الفيروس المتحول**: كما هو الحال مع الفيروس متعدد الأشكال ، يتحور الفيروس المتحور مع كل إصابة. الفرق هو أن الفيروس المتحول يعيد كتابة نفسه بالكامل عند كل تكرار ، مما يزيد من صعوبة اكتشافه. قد تغير الفيروسات المتحولة سلوكها وكذلك مظهرها.

1- البرمجيات الضارة : أ - الفيروسات : الخصائص

هناك عدّة خصائص لفيروسات الحاسب الآلي تميزها من غيرها من البرامج الضارّة، وتساعدها على الانتشار وإصابة أجهزة الحاسب الآلي دون علم مستخدميها، وهي:

- التخفّي: ويعني القدرة على الارتباط ببرامج أو ملفّات أخرى تبدو سليمة ومألوفة للمستخدم، بحيث يلحق الفيروس نفسه بالملف المصاب خفية ليصبح جزءًا منه. ومن أشهر طُرُق تخفي الفيروسات ما يلي:
  - التخفّي في مرفقات البريد الإلكتروني.
  - التخفّي في الملفّات التي يجري تحميلها من مواقع الإنترنت، خاصّة تلك التي تشغّل ملفات الصوتيات والفيديو وتتبادلها.
  - التخفي وراء الروابط والأوامر الموجودة في صفحات الإنترنت والبريد الإلكتروني.
  - التخفّي وراء روابط وملفات الإعلانات والبريد الدعائي.
  - التخفّي مع البرامج المنسوخة بشكل غير قانوني.

1- البرمجيات الضارة : أ - الفيروسات : الخصائص

- التضاعف: ويعني ذلك أن ينسخ الفيروس نفسه عدّة نسخ تصل في بعض الأحيان إلى ملايين النسخ، بمعنى أنه يتكاثر ليصيب أكبر قدر ممكن من الملفّات والبرامج داخل جهاز الحاسب الآلي نفسه أو داخل الأجهزة الأخرى المرتبطة به. وتبدأ عمليّة التضاعف عندما يتم تحميل برنامج الفيروس إلى ذاكرة الحاسب الآلي وينفّذه المعالج المركزي.
- الانتشار: ويعني انتقال الفيروس من جهاز إلى آخر عبر شبكات الحاسب الآلي أو وسائط التخزين المختلفة، ومعنى ذلك أنّ لدى الفيروس القدرة على نقل نفسه عند استثارته، كتشغيل أمر النسخ، أو عند اكتشاف اتصال الحاسب الآلي المصاب بحاسب آلي آخر، ومن أشهر طُرُق انتشار الفيروسات ما يلي:
  - تحميل ملفات مصابة من مواقع شبكة الإنترنت أو زيارة مواقع تنشر الفيروسات بشكل تلقائي.
  - فتح مرفقات بريد إلكتروني مصابة.
  - أن ينسخ المستخدم ملفات مصابة دون علمه، ويخزّنها على وسائط تخزين خارجية تنتشر معها، أو يرسلها عبر الشبكة(كاستخدام المجلّدات المشتركة)، فتنتشر عبرها.

1- البرمجيات الضارة : أ - الفيروسات : الانواع

- فيروسات قطاع بدء التشغيل(الإقلاع) : يوجد لكل نظام تشغيل قطاع في قرص التخزين الصلب، مخصّص لبدء عمليّة التشغيل(الإقلاع) وعادة ما يكون هذا القطاع هو القطاع الأول(Track 0) ، وعند وجود أيّ خلل فيه فإنّ الحاسب الآلي لن يستطيع البدء بالتشغيل. وفيروسات قطاع بدء التشغيل(Boot Sector Viruses) هي الفيروسات التي تصيب قطاع بدء التشغيل في قرص التخزين الصلب، وتكمن خطورة هذا النوع من الفيروسات في إصابتها لمكان مهم جدًّا يتم من خلاله توجيه الجهاز لتنفيذ البرامج التي يجري من خلالها استكمال تجهيز جهاز الحاسب الآلي للعمل، وبدلًا من ذلك يوجّه الفيروس الحاسب الآلي لتنفيذ الكود الخاص بالفيروس، و من ثَمَّ يفشل الجهاز في عمليّة الإقلاع ولا يمكنه العمل.
- فيروسات الملفّات(File Infecting Viruses) : هي الفيروسات التي تصيب الملفّات بشتى أنواعها؛ فيمكن أن تصيب ملفّات نظام التشغيل كملف(Command.com) في نظام الويندوز أو أيّ ملف آخر، وعادة ما ينتج عن هذه الفيروسات زيادة في أحجام الملفّات.

1- البرمجيات الضارة : أ - الفيروسات : الانواع

- الفيروسات الجزئيّة الكبيرة: تستخدم الفيروسات الجزئيّة الكبيرة(Macro Viruses) البرمجة الجزئية الخاصة بتطبيق معيّن، مثل معالج الكلمات، للبدء بنشاطها. وتضرب هذه النوعيّة من الفيروسات ملفات البيانات(مثل ملفات برامج وورد وإكسل وأكسس) ، وتظل ساكنة أو مقيمة في التطبيق نفسه عن طريق إصابة حقل التهيئة الخاص به. وعلى الرغم من أنّ الفيروسات الجزئية الكبيرة تصيب ملفات البيانات، إلا أنّها عمومًا لا تعدّ من فيروسات الملفّات، والسبب في ذلك أن فيروسات الملفّات قد تصيب البرامج وملفات البيانات، بينما لا تصيب فيروسات الجزئية الكبيرة إلا ملفات البيانات فقط.
- فيروسات البريد الإلكتروني: هي الفيروسات التي تنتقل بوساطة البريد الإلكتروني. فبإضافة بعض الوظائف(عن طريق الفيروس) لبرنامج مقدم خدمة البريد الإلكتروني القياسي(مثل أوتلوك(Outlook)) أصبح للفيروسات إمكانية الانتشار عبر العالم خلال ساعات فقط، بدلًا من شهور. ومن أشهر فيروسات البريد الإلكتروني فيروس ماليسا(Melissa) وماليسا ليس أول فيروس بريد إلكتروني، بل أول فيروس بريد إلكتروني انتشر بنجاح بصورة شرسة هو فيروس كريستما إكسك(Christma Exec) في خريف ١٩٨٧م

1- البرمجيات الضارة : أ - الفيروسات : الأعراض

عندما يصاب جهاز الحاسب الآلي بفيروس فإنّه قد يظهر عليه بعض الأعراض الآتية:

- البطء الشديد: يعمل الحاسب الآلي ببطء ملحوظ، وتصبح سرعة البرامج المركبة عليه أبطأ من المعتاد، ومن ذلك أن نظام التشغيل يعمل ببطء شديد عند بداية التشغيل، أو عند إيقاف التشغيل، وقد يكون سبب هذا البطء هو النقص الشديد في الذاكرة العشوائية(RAM).
- تعليق(أو تجمد) الحاسب الآلي: يدخل الحاسب الآلي في حالة من الجمود وعدم الاستجابة لأيّ أمر؛ فلا يمكن في هذه الحالة تشغيل أيّ برنامج، أو حتى إيقاف عمل الجهاز.
- انهيار الحاسب الآلي: في أغلب حالات انهيار الحاسب الآلي تظهر شاشة غريبة(كالشاشات الزرقاء في نظام التشغيل ويندوز)، وعندئذ يتوقف الحاسب الآلي عن العمل.
- إضاءة لمبة القرص الصلب بشكل عشوائي ومتّصل.
- زيادة أحجام الملفّات وزيادة الزمن اللازم لفتح الملفّات أو تشغيل البرامج.
- وجود بيانات تالفة كانت صالحة من قبل.
- ظهور رسائل خطأ، ومربعات حوار غير مألوفة وغير متوقعة.
- إعادة تشغيل الحاسب الآلي بشكل آلي ومستمر دون تدخل المستخدم.

1- البرمجيات الضارة : ب - ديدان الحاسب الالى

دودة الحاسب الآلي(Worm Computer) هي عبارة عن برنامج مستقل بذاته، وله ملف خاص به. فالدودة تُعدُّ برنامجًا تطبيقيًّا متكاملًا يمكن أن يعمل لوحده، ولا يحتاج لأن يضيف نفسه لملف آخر، كما هي الحال في الفيروسات. ويمكن للدودة أيضًا أن تعمل بمفردها وتحمّل نفسها إلى ذاكرة الحاسب الآلي، وتبدأ بالعمل بشكل آلي.

من الفوارق الأصليّة، هي أن الديدان تستخدم الشبكات وروابط الاتصالات لكي تنتشر، وهي خلافًا للفيروسات لا تلتحم مباشرة بالملفّات القابلة للتنفيذ. وتصيب الديدان أجهزة الحاسب الآلي المرتبطة بشبكات الحاسب الآلي المصابة دون تدخل المستخدم أو قيامه باستثارتها كفتح ملف معين أو تشغيل برنامج، كما هي الحال في الفيروسات. فقد تنتقل إلى الجهاز بمجرّد تصفّح بعض مواقع الإنترنت، أو بمجرّد فتح بريد إلكتروني(إذا لم يكن الجهاز محميًا ببرنامج حماية محدّث) وهذا الأمر يجعلها تنتشر بشكل أسرع وأوسع من الفيروسات.

برنامج الدودة يتكوّن من أجزاء(رأس وجسم كما في الدودة الطبيعية) تعمل في أجهزة حاسب متفرقة، تتواصل فيما بينها عبر الشبكة، فيمكن أن تجد رأس البرنامج في جهاز، وذيله في جهاز آخر بعيد.

1- البرمجيات الضارة : ب - ديدان الحاسب الالى : الخصائص

من أهم خصائص الديدان هي قدرتها على الانتشار والتكاثر عبر الاتصال بشبكات الحاسب الآلي، ومن أهم الطرق التي تنتشر بها الديدان ما يلي:

- مرفقات البريد الإلكتروني المصابة.
- التحميل التلقائي عند زيارة بعض مواقع الإنترنت التي من خلالها تنتشر الديدان، أو عند استخدام أحد الارتباطات داخل البريد الإلكتروني.
- التسلل عبر الثغرات الأمنيّة في أنظمة التشغيل أو برامج الحماية.
- أضرار الديدان

- لا تقل أضرار الديدان عن الفيروسات من ناحية التلف، أو فقْد البيانات التي تسببها، ومن أهم أضرار الديدان ما يلي:
- تتيح للمهاجم أن يستخدم الحاسب الآلي المصاب لمهاجمة أجهزة أخرى، أو مواقع الإنترنت، أو إرسال بريد إلكتروني، أو تحميل برامج ضارّة إليه.
- يمكن من خلالها فتح باب خلفي(Back Door) في الجهاز المصاب، حيث يمكن التحكّم به من خلال ذلك الباب.
- يمكن للديدان أن تنسخ نفسها، وترسل نسخة إلى كل بريد إلكتروني في عناوين البريد المخزّنة في جهاز الحاسب الآلي المصاب.

1- البرمجيات الضارة : ب - ديدان الحاسب الالى: التقنيات الحالية للدودة

تشمل أحدث تقنيات الدودة ما يلي:

- **منصات متعددة**: لا تقتصر الديدان الأحدث على أجهزة ويندوز ولكن يمكنها مهاجمة مجموعة متنوعة من الأنظمة الأساسية ، وخاصة الأنواع الشائعة من يونيكس.
- **استغلال متعدد**: تخترق الديدان الجديدة الأنظمة بعدة طرق ، وذلك باستخدام عمليات الاستغلال ضد خوادم الويب والمتصفحات والبريد الإلكتروني ومشاركة الملفات والتطبيقات الأخرى المستندة إلى الشبكة.
- **الانتشار فائق السرعة**: تتمثل إحدى تقنيات تسريع انتشار الدودة في إجراء فحص مسبق للإنترنت لتجميع عناوين الإنترنت الخاصة بالأجهزة المعرضة للخطر.
- **متعدد الأشكال**: لتفادي الاكتشاف وتخطي المرشحات واحباط التحليل فى الوقت الحقيقي ، تعتمد الديدان تقنية الفيروسات متعددة الأشكال. تحتوي كل نسخة من الدودة على رمز جديد يتم إنشاؤه سريعًا باستخدام تعليمات وتقنيات تشفير متكافئة وظيفيًا.
- **المتحولة**: بالإضافة إلى تغيير مظهرها ، تمتلك الديدان المتحولة حزمة من أنماط السلوك التي يتم إطلاقها في مراحل مختلفة من التكاثر.
- **مركبات النقل**: نظرًا لأن الفيروسات المتنقلة يمكنها اختراق عدد كبير من الأنظمة بسرعة ، فهي مثالية لنشر أدوات الهجوم الموزعة الأخرى ، مثل التعطيل الموزع للخدمة.
- **استغلال يوم الصفر**: لتحقيق أقصى قدر من المفاجأة والانتشار ، يجب أن تستغل الدودة ثغرة غير معروفة و لم يتم اكتشافها إلا عند إطلاق الدودة.

1- البرمجيات الضارة : ج – برامج احصنة طروادة

في مجال أمان الحاسب الآلي، يعرّف حصان طـروادة بأنّه جزء من برنامج(كود) قابل للتنفيذ يؤدي بعض المهام لا يتوقعها المستخدم، ويقيم في البرنامج المصاب. وطروادة يمكن أن يوضع في برنامج بريء عنـد تأليفه وجمعه، أو يمكن إضافته للبرنامج بعد جمعه. وسبب تسمية هذا البرنامج الضار بهذا الاسم هو تشابه عمله مع أسطورة الحصان الخشبي الذي اختبأ به عدد من الجنود اليونانيين، وكانوا سببًـا في فتح مدينة طروادة[1]. فبرنامج حصان طروادة هو برنامج ضار(الجنود)، مختبئ داخل برنامج بريء(حصان خشبي).

إنّ مصطلح حصان طروادة يحمل في طيّاته دلالة سالبة جدًّا، بسبب وفرة أحصنة طروادة المنتشرة، التي صُمّمت بغرض إغراق أجهزة الكمبيوتر. وعلى الأقل يمكن لحصان طروادة ألا يكون أكثر من مجرد إزعاج، وفي أسوأ مراحله يمكن لحصان طروادة أن يدمّر بالكامل عمل الجهاز الذي يسكنه.

1- البرمجيات الضارة : ج – برامج احصنة طروادة

عمومًـا يمكـن تقسيم برامـج حصان طـروادة إلـى تلك التـي تنتشر عـن طريق تغيير شيفرة(كود) المصدر(Source Code)، وتلك التي تنتشـر عن طريق إصابة الملف القابل للتنفيذ يدويًّا. وطريقة الانتشار السابقة تفترض أنّ لدى مؤلّف حصان طروادة لديه القدرة على تحوير شيفرة المصدر لكي تحتوي برنامج حصان طـروادة، وأنّ لديه القدرة بعد ذلك على جمـع البرنامج البريء ونشره، وهذا الخيـار لا يكون دائما ممكنًـا، ولذلك فإنّ مؤلفي أحصنة طروادة قد يلجؤون في بعض الأحيان لتحوير الملفّات الموجودة مسبقًا والقابلة للتنفيذ. والبرامج التي يجري تحويرها بهذه الطريقة هي البرامـج العامّة، التي توفّر بغرض تحميل برامج أخرى، أو برامج نظم التشغيل التي تكون في الجهاز محل الهجوم.

تختلف أحصنة طروادة عن فيروسات وديدان الحاسب الآلي بأنها لا تتكاثر أو تتضاعف. ففيروسات الحاسب الآلي هي برامج تتضاعف عن طريـق إصابة البرامج الأخرى، وتحتاج إلى استثارتها من قبل المستخـدم لكي تنتشر، والديدان قد تصيـب البرامج التنفيذية أو لا تصيبها، ولا تتطلّب عـادة استثارتها من قبل المستخدم بصورة واضحـة لكي تتضاعف، إلا أنّها تتضاعف وتنتشر بطريقة أسرع من الفيروسات. وقد ظهر الفرق بين الفيروس والدودة بمرور السنوات، لكن الفارق الرئيس بينهما وبين حصان طروادة هو أنّ هذا الأخير لا يتكاثر.

1- البرمجيات الضارة : د – المكافحة

يمكن مكافحة البرامج الضارّة باستخدام حزمة برامج واحدة لمكافحة كل من الفيروسات والديدان وأحصنة طروادة في آن واحد؛ لذا لا بدّ من تثبيت برنامج مكافحة جيّد وتحديثه دوريًّا لتوفير الحماية المطلوبة. ولا بدّ أن تشتمل برامج الحماية ليس فقط على كشف الإصابات فقط، وإنّما إزالتها أيضًا، وهناك عدّة برامج(أو حزم) مشهورة لمكافحة البرامج الضارّة يمكن الاعتماد عليها، ومن أشهرها:

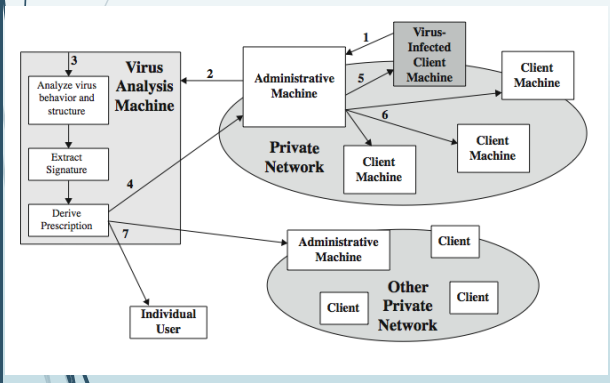
- حزمة برامج مكافي(McAfee).
- حزمة برامج سيمانتك(Symantec).
- حزمة برامج كاسبر سكاي(Kasper SKY).
- حزمة برامج نورتون(NORTON).
- وفي جميع الحالات لا بدّ من اتّباع الخطوات الآتية للحصول على مكافحة جيدة:
- تحديث برنامج المكافحة آليًّا ودوريًّا لضمان كشف الفيروسات والديدان وأحصنة طروادة الحديثة ومنعها.
- تحديث نظام التشغيل آليًّا ودوريًّا عن طريق تنشيط خاصية التحديث التلقائي لسد الثغرات الأمنيّة عند ظهورها.

1- البرمجيات الضارة : د – المكافحة

- تحميل ملفات الإصلاح الأمنيّة الخاصة بأنظمة التشغيل وبعض البرامج التطبيقيّة الأخرى،(كحزمة برامج الأوفيس) التي تصدرها الشركات المصنّعة(كشركة مايكروسوفت) بشكل مستقلّ لسدّ ثغرة أمنيّة خاصّة لم يتم سدها من خلال التحديث التلقائي، وكذلك تحميل حزم الخدمة(Service Pack) الجديدة حال ظهورها.
- عدم فتح مرفقات البريد الإلكتروني التي لها الامتدادات التشغيليّة مثل:(scr) (exe vbs)، أو التي لها أكثر من امتداد مثل(txt.vbs).
- ويمكن أن تعمل برامج المكافحة بإحدى الطرق الآتية أو جميعها:
- باستخدام جدول زمني معيّن يحدّد من خلاله عمل برنامج المكافحة؛ ليبدأ بفحص جميع مكوّنات الجهاز عند أوقات محدّدة(عند منتصف الليل من كل يوم مثلًا).
- عند الطلب من قبل المستخدم، ويمكن أن يكون ذلك في أيّ وقت.
- عند تشغيل البرامج أو فتح الملفّات أيًّا كان نوعها، وفي هذه الحالة يفحص برنامج المكافحة الملف المراد فتحة قبل أن تتم عمليّة الفتح الفعليّة؛ للتأكد من خلوّه من الفيروسات والديدان وأحصنة طروادة، ومن الأفضل تفعيل جميع هذه الطرق لتوفير حماية أفضل وأشمل.

1- البرمجيات الضارة : نظام المناعة الرقمي

نظام المناعة الرقمي هو نهج شامل للحماية من الفيروسات طورته شركة IBM وصقلته لاحقًا شركة (Symantec). الهدف من هذا النظام هو توفير وقت استجابة سريع بحيث يمكن القضاء على الفيروسات بمجرد دخولها.



عندما يدخل فيروس جديد إلى نظام ما ، يلتقطه النظام المناعي تلقائيًا ويحلله ويضيف الكشف والوقاية منه ويزيله ويمرر معلومات حول هذا الفيروس إلى أنظمة أخرى بحيث يمكن اكتشافه قبل السماح له بالعمل في مكان آخر ، كما يوضح الشكل:

IBM/Symantec Project

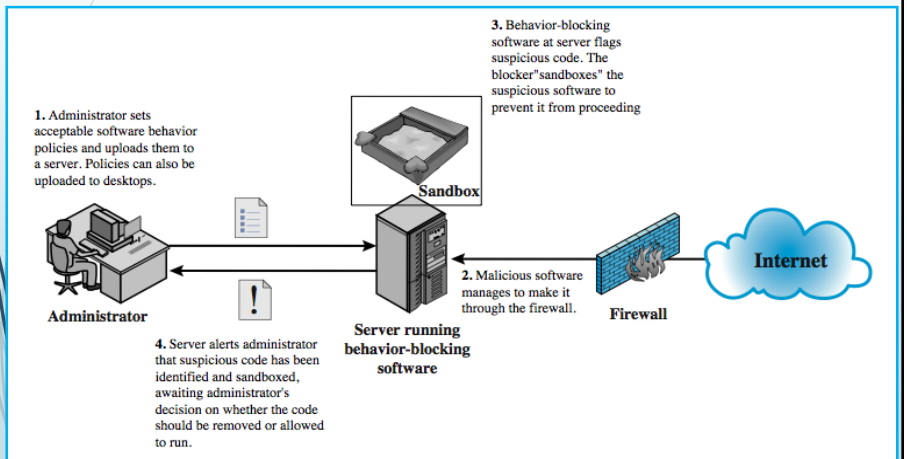
1- البرمجيات الضارة : نظام المناعة الرقمي

1. يستخدم برنامج المراقبة على كل حاسوب مجموعة متنوعة من الأساليب التجريبية لاستنتاج وجود فيروس ، ويعيد توجيه نسخة إلى جهاز مشرف النظام.
2. يقوم حاسوب مشرف النظام بتشفير الفيروس وإرساله إلى حاسوب تحليل الفيروسات المركزي.
3. ينشئ هذا الجهاز بيئة يمكن فيها تشغيل البرنامج المصاب بأمان للتحليل. ثم يصدر حاسوب تحليل الفيروسات وصفة طبية لتحديد الفيروس وإزالته.
4. يتم إرسال الوصفة الطبية الناتجة إلى حاسوب المشرف.
5. يقوم حاسوب المشرف بإرسال الوصفة الطبية إلى العميل المصاب.
6. يتم إرسال الوصفة الطبية أيضًا إلى عملاء آخرين في النظام.
7. يتلقى المشتركون في جميع أنحاء العالم تحديثات منتظمة لمكافحة الفيروسات لحمايتهم من الفيروسات الجديدة.

يعتمد نجاح جهاز المناعة الرقمي على قدرة حاسوب تحليل الفيروسات على اكتشاف سلالات فيروسية جديدة ومبتكرة. من خلال التحليل المستمر للفيروسات الموجودة في بيئة العمل ومراقبتها ، يجب أن تكون هناك امكانية تحديث برمجيات المناعة الرقمية باستمرار لمواكبة التهديدات.

1- البرمجيات الضارة : برنامج حظر السلوك

برنامج حظر السلوك هو متكامل مع نظام تشغيل الحاسب المضيف ويراقب سلوك البرنامج في الوقت الفعلي بحثًا عن الإجراءات الضارة. يقوم برنامج حظر السلوك بعد ذلك بحظر الإجراءات التي يحتمل أن تكون ضارة قبل أن تؤثر على النظام.



1- البرمجيات الضارة : برنامج حظر السلوك

يمكن أن تشمل السلوكيات المراقبة

- محاولات فتح الملفات وعرضها وحذفها و / أو تعديلها ؛
- محاولات تهيئة محركات الأقراص وعمليات القرص الأخرى غير القابلة للاسترداد ؛
- تعديلات على منطق تنفيذ الملفات أو وحدات الماكرو ؛
- تعديل إعدادات النظام الهامة ، مثل إعدادات بدء التشغيل ؛
- برمجة عملاء البريد الإلكتروني والمراسلة الفورية لإرسال محتوى قابل للتنفيذ ؛
- بدء اتصالات الشبكة.

يوضح الشكل عملها. يتم تشغيل برنامج حظر السلوك على أجهزة حاسوب الخادم وسطح المكتب ويتم توجيهه من خلال السياسات التي وضعها مسؤول الشبكة للسماح بتنفيذ الإجراءات الحميدة ولكن للتدخل عند حدوث إجراءات غير مصرح بها أو مشبوهة. تمنع الوحدة أي برامج مشبوهة من التنفيذ. يعزل برنامج الحظر البرنامج المنفذ في وضع الحماية ، مما يقيد وصوله ال إلى موارد وتطبيقات نظام التشغيل المختلفة. ثم يرسل برنامج الحظر التنبيه. نظرًا لأن أداة حظر السلوك يمكنها حظر البرامج المشبوهة في الوقت الفعلي ، فإنها تتمتع بميزة على تقنيات الكشف عن الفيروسات الراسخة مثل البصمات أو الاستدلال. حظر السلوك وحده له حدود. نظرًا لأنه يجب تشغيل الشفرة الخبيثة على الجهاز الهدف قبل التعرف على جميع سلوكياتها ، فقد تتسبب في حدوث ضرر قبل اكتشافها وحظرها.

2 - برمجيات التجسس:-

لقد عُرفت فيروسات الحاسب الآلي بصـورة موسعة في أواخر الثمانينيّات. فهي كائنات غريبة ولافتة للنظر، وفي كل مرة يوجّه الفيروس ضرباته يكـون هو موضوع الأخبار، خاصّة إذا انتشـر بسرعة. وخلال السنوات القليلة الماضية ظهرت فئـة جديدة من البرامج الماكرة هي برامج التجسّس، وبرنامج التجسّس ليس بفيروس، لكن فعله أقوى وأخطر من الفيروسات والديدان وأحصنة طروادة. فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يفعل فعله من وراء الكواليس بكل هدوء، ودون علم المستخدم، وينقل المعلومات لمالكه. وبرنامج التجسّس هو عبارة عن خدعة ماكرة، مثله في ذلك مثل الفيروس، لكنه عمومًا أقل شهرة.

على الرغم من الجدل الذي يكتنف تعريف برنامج التجسّـس الدقيق، إلا أنّه في النهاية كائن (إلكتروني) يتجسّس عليك، ونتيجة لذلك يتركز الجانب المهم من موضوع برنامج التجسّس عادةً حول مسألة الخصوصيّة. ويُعـدُّ تعريف ويبوديا[٢] لبرنامج التجسّـس أفضل التعريفات الموجودة، حيث عرّفه بأنه: «أيّ برنامج يحصل –سرًّا– على معلومات عن المستخدم عن طريق الربط بالإنترنت، وخاصة بدعاوى دعائية وإعلانيـة». عادةً ما يتم تضمين برامج التجسّس في شكل مكوّنات مجانيّة خفية، أو برامج مشاركة يمكن تنـزيلها من شبكة الإنترنت، وبمجرّد تركيب برنامج التجسّس يبدأ بمراقبة حركة المستخدم علـى الإنترنت، وينقل المعلومات من وراء الكواليس لجهة أخرى.

2 - برمجيات التجسس:- الانواع

كما رأينا في تعريف برامج التجسّس، فهي برامـج خطيرة تتسلل إلى الحواسيب وتعرف المعلومـات الخاصة والسِّريّة المخزّنة بها، وربما ترسلها إلـى أجهزة أخرى بمجرد توفر خط الاتصال، وبناءً على طريقة عملها، يمكن تصنيف برامج التجسّس إلى نوعين رئيسين: برامج رصد وتسجيل، وبرامج تتبع.

النوع المعروف من برامج الرصد والتسجيل هو مسجل أو راصد المفاتيح (من لوحة المفاتيح) وحركات الفأرة. فهو يعمل في صمت في الخلف ويقوم بتسجيل ضغطات المفاتيح وحركات الفأرة لكي يعيد ترتيب وتكوين ما يفعله المستخدم، وهـذه الطريقة شديدة الخطورة، إذ يمكن من خلالها معرفة الأرقام السِّريّة أو الأرقام الخاصة التي يُدخلها المستخدم عبر لوحة المفاتيح. وخلافًا لراصد عمل المفاتيح، هناك أيضًا راصدات ومسجلّات للبريد الإلكتروني والدردشة. وراصدات عمل المفاتيح مشهورة؛ لأنّها هي أكثر الأنواع شيوعًا وإزعاجًا في عمليّة سرقة كلمات السر وأرقام بطاقات الائتمان.

أمّا المتتبّعات فتراقب عادات الاستخدام وأنماطه وتخزّنها كبيانات إحصائيّة بهدف إعداد التقارير بناءً عليها. وقد تكون البيانات عبارة عن عادات التصفح للشخص المستهدف، مثل استخدام برنامج معيّن أو خاصية محدّدة في ذلك البرنامج. ويتم تجميع هذه المعلومات عن الشخص الضحية ثم تحليلها واستخدامها في الهجوم عليه أو سرقة معلوماته.

2 - برمجيات التجسس:- طريقة العمل

فنيًّا لا يصنف برنامج التجسّس كفيروس، ولذلك لا يمكن مكافحته بشكل كامل من خلال البرامج المصمّمة لمكافحة الفيروسات. وعلى وجه التحديد تُتلف الفيروسات البيانات على جهاز الحاسب الآلي وتنسخ نفسها ذاتيًّا، في حين تعمل برامج التجسّس خلسة، ولا تتلف البيانات، بل تتجسّس عليها. ويمكن لبرامج التجسّس أن تنسخ نفسها على الجهاز وتعمل كمهمة خلفية، ثم تنقل المعلومات السِّريّة الخاصة بالمستخدم لمالكها دون علم المستخدم.

لدى برنامج التجسّس مكوّنان أساسيّان: ففي الواجهة الأمامية هو برنامج عادي يعمل في العلن، ويوفر وظائف مفيدة، بينما هو في الخلف برنامج تجسّس يراقب وينقل المعلومات. ويمكن لبرنامج التجسّس البقاء في أيّ صورة أو شكل من أشكال البرامج القابلة للتنفيذ، بما في ذلك التطبيقات مثل (ActiveX. Plug-in)، أو أكواد (Applets).

عادة لا تجمع برامج التجسّس المعلومات الشخصيّة فقط، لكن بالإضافة إلى ذلك تجمّع المعلومات الديموغرافية وعادات التصفح. ومن المحتمل أن تباع هذه المعلومات المتحصل عليها، أو أن تضاف لقواعد البيانات الأخرى لبناء سجلّات عن المستخدم وعادات استخدامه، وعن طريق ربطها بالبيانات الشخصية، مثل: الاسم والعنوان وعنوان البريد الإلكتروني والعمر والجنس والدخل وتاريخ الائتمان، قد تكون من أقوى وسائل التسويق. ومن الطبيعي أن يكون

2 - برمجيات التجسس:- طريقة العمل

لها بعض الأعراض، ومنها:

- نشاط أعلى من الحد المعتاد: ويتضح ذلك أكثر عندما يرسل الحاسب الآلي ويستقبل كميّات كبيرة من البيانات عبر الشبكة أو الإنترنت، في حين أن المستخدم لا يستخدم أيّ برامج تستوجب ذلك، ويمكن ملاحظة ذلك عن طريق مراقبة عمل جهاز المودم وعرض كميّة البيانات التي أرسلها واستقبلها.
- طلب الاتصال بالإنترنت تلقائيًا: وتظهر هذه الحالة في الأجهزة التي لا يوجد بها جهاز مودم (Digital Subscriber Line-DSL)، حيث يشغّل برنامج التجسّس طلب الاتصال الهاتفي من أجل الارتباط بالإنترنت.
- ظهور أشرطة أدوات غير مألوفة تُضاف إلى متصفّح الإنترنت.
- اختيار صفحة بداية لمتصفّح الإنترنت خلاف الصفحة التي تم ضبط المتصفّح عليها من قبل المستخدم.

ومن أشهر الطرق التي تنتقل بها برامج التجسّس طريقتان، هما:

- تظهر كأنها برامج عادية حتى يتم تثبيتها من قبل المستخدم وبعلمه.
- الاختفاء في برامج أخرى، بحيث يجري تثبيتها مع هذه البرنامج دون علم المستخدم.

2 - برامج التجسس:- المكافحة

من أخطر ما تفعله برامج التجسّس هو أنها تُزيل برامج مكافحة التجسّس. ويمكن القول إنّه ليس هناك برنامج يحمي من برامج التجسّس بدرجة كاملة، لكن يمكن أخذ بعض التدابير الوقائية، ومنها:

- مصفيات خاصية استرجاع البيانات
- حاجبات الاعلانات و النوافذ المنبثقة
- استخدام مضادات برامج التجسس
- استخدام جدار النار الشخصي و برامج كشف التطفل
- تأمين متصفح الانترنت
- تأمين ادخال كلمات المرور

3 – أمن انظمة التشغيل و الملفات

هناك أربعة عناصر رئيسة يمكن من خلالها تحقيق الحد الأدنى لأمن أنظمة التشغيل والملفّات، وهي:

١. التحقّق من الهُويّة: يتطلب ذلك أن تكون أصول أجهزة الحاسب الآلي(أنظمة التشغيل، والملفّات، والأجهزة نفسها) قادرة على التحقّق من هويّة المستخدم، ومن هويّة البرامج والبيانات.

٢. السِّريّة: وتتطلب أن يكون الدخول إلى أنظمة الحاسب الآلي والبيانات المخزّنة بها من قبل الجهات المصرّح لها فقط، وأن تبقى البيانات والمعلومات سرّيّة(غير مقروءة) لمن ليس له حق الاطّلاع عليها. وفي أنظمة التشغيل تكون المعلومات السِّريّة للقراءة فقط من قبل الجهات المصرّح لها بذلك فقط، وهذا النوع من الدخول يشمل: الطباعة، والعرض، وأنواع الاستعراض(التصفح) الأخرى، وكذلك يشمل إمكانية الكشف عن وجود العنصر(ملف أو مجلد مثلًا).

٣. السلامة والتكاملية: ويتطلب ذلك إمكانية تعديل أصول أنظمة الحاسب الآلي بوساطة الجهات المصرّح لها بذلك فقط، والتعديل يشمل: الكتابة، والتغيير، وتغيير الوضع، والحذف والإنشاء.

٤. التوافر: يتطلب ذلك أن تكون أصول أنظمة الحاسب الآلي متوافرة للجهات المخول لها باستخدامها.

3 – أمن انظمة التشغيل و الملفات

وتهدف هـذه العناصر في مجملها إلى تحقيق الغايات الآتية، التي تُعدُّ هي جوهر أمن أي نظام تشغيل:

- ضبط الدخول: ويهتم هذا بتنظيم دخول المستخدم إلى كامل نظام التشغيل، والأنظمة الفرعية والبيانات، وينظّم عمليّة الدخول إلى مختلف الموارد في النظام.
- ضبط تدفق المعلومات: ينظّم تدفق البيانات في النظام وتسليمها إلى المستخدمين .
- التأكيد: يتعلّق بإثبات أنّ الدخول وآليات ضبط التدفق تعمل وفقًا لمواصفاتها، وأنّها تفرض الحماية المطلوبة والسياسات الأمنيّة.